

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD W. NAGEL
CLERK OF COURT

1/19/21

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Information associated with the email address
wenglebot@yahoo.com that is stored at premises
controlled by Oath Holdings Inc.

Case No. 3:21MJ26

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WEST. DIV. DAYTON

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-2

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B-2

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

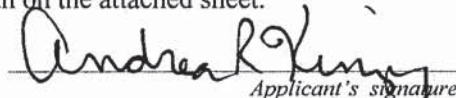
Code Section

SEE ATTACHMENT C-2

Offense Description

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature
Andrea R. Kinzig, FBI Special Agent
Printed name and titleAttested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone _____ (specify reliable electronic means).

Date: 1/19/21

City and state: Dayton, OH

U.S. Magistrate Judge
Name and title

ATTACHMENT A-2

Information associated with the email address **wenglebot@yahoo.com** that is stored at premises controlled by Oath Holdings Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California, 94089.

ATTACHMENT B-2
Particular Things to be Seized

I. Information to be disclosed by Oath Holdings Inc. (the “Provider”)

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. The types of service utilized;
4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Cloy Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider’s electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography), and 21 U.S.C. §844 (possession of controlled substances) involving WILLIAM HITCHINGS from January 1, 2019 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Any records related to the possession of controlled substances.
9. Any images or videos depicting controlled substances and drug paraphernalia (such as scales, packaging materials, bongs, etc.).
10. Any communications about the purchase, acquisition, sale, or transfer of controlled substances.
11. Evidence of utilization of telephone accounts, Internet Service Providers, and financial accounts, including but not limited to monthly billing statements;
12. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
13. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-2

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
21 U.S.C. §844	Possession of Controlled Substances

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of suspected child pornography and drug offenses committed by WILLIAM SIDNEY HITCHINGS V (hereinafter referred to as "HITCHINGS"). This Affidavit is submitted in support of Applications for search warrants for the following:
 - a. Information associated with the Google account associated with the email addresses **w.hitchings@gmail.com** and **wenglebot@yahoo.com** that is stored at premises controlled by Google LLC (as more fully described in Attachment A-1);
 - b. Information associated with the email address **wenglebot@yahoo.com** that is stored at premises controlled by Oath Holdings Inc. (as more fully described in Attachment A-2);
 - c. Information associated with the Skype account containing the user name of **o0bc0o** and/or associated with the email address **w.hitchings@gmail.com** that is stored at premises controlled by Microsoft Corporation USA (as more fully described in Attachment A-3); and
 - d. Information associated with the Dropbox account associated with the email address **w.hitchings@gmail.com** that is stored at premises controlled by Dropbox Inc. (as more fully described in Attachment A-4).
3. The purpose of the Applications is to search for and seize evidence of suspected violations of the following:
 - a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography;

- b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce;
 - c. 21 U.S.C. § 844, which make it a crime to possess controlled substances
- 4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-4 hereto and are incorporated by reference.
 - 5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
 - 6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 through A-4).
 - 7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and property designed for use, intended for use, or used in committing a crime of violations of federal law; including violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(1), 18 U.S.C. §§ 2252(a)(2) and (b)(1), 18 U.S.C. §§ 2252A(a)(2) and (b)(1), and 21 U.S.C. § 844, are present in the information associated with the above noted accounts (as described in Attachments A-1 through A-4).

JURISDICTION

- 8. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

- 9. 18 U.S.C. § 2252(a)(2) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such

visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

10. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
11. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
12. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
13. 21 U.S.C. § 844 states that it is a violation for any person to knowingly or intentionally possess a controlled substance unless such substance was obtained directly, or pursuant to a valid prescription or order, from a practitioner, while acting in the course of his professional practice, or except as otherwise authorized by this subchapter or subchapter II of this chapter.

BACKGROUND INFORMATION

Definitions

14. The following definitions apply to this Affidavit and Attachments B-1 through B-4 to this Affidavit:

- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).
- e. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- f. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- g. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up

Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

- h. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- i. **“Social Media”** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users’ account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.
- j. **“Exchangeable image file format”**, also referred to as **“EXIF data”**, is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners, and other systems handling image and sound files stored by digital cameras. Most new digital cameras use the EXIF annotation, storing information on images such as shutter speed, exposure compensation, F number, metering system used, if a flash was used, ISO number, date and time the image was taken, etc.
- k. **“Metadata”** is data that provides information about other data. For computer files, metadata can be stored within the file itself or elsewhere. Metadata for computer files includes the file name, the file type, where it is stored (*i.e.*, the file path), when it was created, when it was last modified and accessed, the file size, and other information.
- l. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs),

Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Collectors of Child Pornography

15. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
 - d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
 - e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography

distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Google Services

- 16. Google LLC is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.
- 17. Google Photos is a photograph and video sharing and storage service provided by Google LLC, located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any cellular telephone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.
- 18. Google+ is a social networking and identity service website owned and operated by Google LLC, located at www.plus.google.com. Common features include the following:
 - a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.
 - b. Circles: Google+ allows users to establish “circles”, which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical “Friends” list function used by sites such as Facebook and MySpace.
 - c. Communities: Communities allow users with common interests to communicate with each other.
 - d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.

- e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.
 - f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.
19. Google Web and App History is a feature of Google Search in which a user's search queries and results and activities on other Google services are recorded. The feature is only available for users logged into a Google account. A user's Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.
20. Google Drive is a file storage and synchronization service provided by Google LLC, located at www.drive.google.com. This service provides cloud storage, file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and other Google services.
21. Google Android Backup is a service provided by Google LLC to backup data connected to users' Google accounts. The service allows users to restore data from any Google account that has been backed up in the event that the users' devices are replaced or erased. Data that can be backed up includes Google Calendar settings, WiFi networks and passwords, home screen wallpapers, Gmail settings, applications installed through Google Play, display settings, language and input settings, date and time, and third party application settings and data.

Email Accounts

22. Google LLC is a multi-national corporation with its headquarters located in Mountain View, California. Oath Holdings Inc. is a company based in Sunnyvale, California. In my training and experience, I have learned that Google LLC and Oath Holdings Inc. provide a variety of online services, including electronic mail ("email") access, to the public.
23. Google LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the accounts listed in Attachment A-1. Oath Holdings Inc. allows subscribers to obtain email accounts at the domain name yahoo.com and ymail.com, like the account listed in Attachment A-2. Subscribers obtain accounts by registering with Google LLC and Oath Holdings Inc. During the registration process, Google LLC and Oath Holdings Inc. ask subscribers to provide basic personal information. Therefore, the computers of Google LLC and Oath Holdings Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC and Oath Holdings Inc. subscribers) and information concerning subscribers and their use of Google LLC and Oath Holdings Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. In general, emails that are sent to Google LLC and Oath Holdings Inc. subscribers are stored in the subscriber's "mail box" on Google LLC's and Oath Holdings Inc.'s servers until the subscriber deletes the email. If the subscriber does not delete the message, the messages can remain on Google LLC's and Oath Holdings Inc.'s servers indefinitely. Even if the subscriber deletes an email, it may continue to be available on Google LLC's and Oath Holdings Inc.'s servers for a certain period of time.
25. Google LLC and Oath Holdings Inc. subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC and Oath Holdings Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
26. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.
27. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.
28. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may

constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

Cloud Storage and Dropbox

30. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:
 - a. “Cloud” is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. “The cloud” was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a

network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.

- b. “Cloud computing” is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- c. “Cloud Service Provider” (CSP) is the entity that offers cloud computing services. CSP’s offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP’s maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP’s reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a “remote computing service.” CSP’s may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.
- d. “Virtual Machine” (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.
- e. “NetFlow Records” are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic

transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.

31. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.'s servers.
32. In general, providers like Dropbox Inc. ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.
33. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.
34. Dropbox Inc. provides its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a "sharing link". A sharing link creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

Skype

35. Skype owns and operates a communication service that transmits voice calls, video, and messages over the Internet. In May 2011, Skype was acquired by Microsoft Corporation, a company based in Redmond, Washington.
36. Skype users can make and receive local, long distance, and international phone calls; participate in video chats or send and receive video messages; send and receive short message system (SMS) text messages; and send and receive electronic files including documents, pictures, audio, and video.

37. Skype may be installed and used on a desktop computer, laptop, tablet, or mobile phone, including those using operating systems from Apple, Blackberry, Google, and Windows.
38. Skype requires users to provide basic contact information to the company during the registration process. This information may include identification data such as name, username, address, telephone number, mobile number, email address, and profile information such as age, gender, country of residence, and language preference.
39. Skype users can elect to make public profile information consisting of images, links to personal web pages, and links to social media websites. Skype users may also subscribe to other Skype users with whom they are interested or associated.
40. When its users communicate with non-Skype users, the company keeps transaction records during the normal course of business commonly referred to as call detail records. These call detail records consist of the date, time, sender, receiver, duration, and contents of phone calls, text messages, and video messages. According to the company, the transactional records are maintained for six months and data files are stored for 30 to 90 days depending on the type of file.
41. In order to use Skype's premium features like voicemail or to make calls to a landline, cellular telephone, or service outside of the Skype network, a customer must either purchase credits or agree to a monthly or otherwise recurring payment option. This necessitates either providing the company with credit card information, including name, billing address, and credit card number, or the use of an online payment processor such as PayPal.
42. Skype retains system information about the types of devices a customer uses to access their service. This can include computer platform and operating system, Internet Protocol (IP) address information, and mobile device information such as device type, manufacturer name, model number, operating system, and cellular service provider.
43. Skype users may elect to import their contacts from email and social media accounts. This contact information can include name, email address, and/or phone numbers.
44. Skype accesses and stores location information regarding its customers. The location information includes Wi-Fi access points when a customer uses Skype from a home or free Wi-Fi spot, global positioning system (GPS) data when a user searches for free Skype Wi-Fi access points, and GPS data when a Skype user shares their location with another user.
45. Skype users can link their social media accounts with the communication provider. These social media accounts may include Microsoft Corporation, LinkedIn, and Twitter. Skype users may also use an associated Microsoft account and other services. These associated services may include online file storage, Microsoft email services, and/or other Microsoft products or services.

46. Skype also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Skype, including the information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.
47. Skype uses the following terms to describe the data in its possession:
 - a. Registration Details: This includes information captured at the time the account was created. This may include identification data such as name, username, address, telephone number, mobile number, email address, and profile information such as age, gender, country of residence, language preference, and any user profile information.
 - b. Billing Address: The billing address provided by the user that is used in conjunction with payment for Skype services.
 - c. Skype Online Current Subscription List: A list of Skype users currently subscribed to by the user.
 - d. Purchase History: Financial transactions with Skype including method of payment information and billing address.
 - e. Skype Out Records: Historical call detail records for calls placed to cellular and landline phone numbers.
 - f. Skype Online Records: Historical call detail records for calls placed to the Skype number from landline and mobile numbers.
 - g. Short Message System Records (SMS): Text messages including the content of the messages.
 - h. Skype Wi-Fi Records: Historical records of connections to Skype Wi-Fi access points.
 - i. Email and Password Records: Historical records of emails and password change activities.
48. Communication providers such as Microsoft Corporation typically retain additional information about their users' accounts during the normal course of business, such as information about the length of service (including start date), the types of services utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Skype users may communicate directly with Skype about issues relating to their accounts, such as technical problems, billing inquiries,

or complaints from other users. Providers like Microsoft Corporation typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

Verizon Cloud

49. Verizon provides cellular telephone access to the general public. Synchronoss Technologies Inc. is a software services company that provides digital, cloud, messaging, and Internet of Things (IoT) platforms to various companies.
50. Verizon allows customers to back up and store the contents of their cellular telephones and tablets to a Verizon Cloud. Contents that can be backed up to the Verizon Cloud include messages, images, videos, documents, contacts, and call logs. The Verizon Cloud allows users to wirelessly back up and synch contents between their cellular telephones, tablets, computers, and other devices.
51. Verizon has a contract with Synchronoss Technologies Inc. to power, administer, and maintain the Verizon Cloud. Synchronoss Technologies maintains the contents of the Verizon Cloud accounts. However, Verizon maintains subscriber information, transactional records, and location information for the telephone accounts.

NCMEC and Cyber Tipline Reports

52. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.
53. As part of its functions, NCMEC administers the Cyber Tipline. The Cyber Tipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the Cyber Tipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities. Many states utilize Internet Crimes Against Children (ICAC) task forces to serve as the intake organizations for the Cyber Tipline reports. These ICAC's review the Cyber Tipline reports received from NCMEC and assign them to the applicable law enforcement agencies. In Ohio, the ICAC in Cuyahoga County serves as this intake organization.

Telegram Messenger

54. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.
55. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.
56. Messages and media in Telegram are client-server encrypted and stored on servers by default. Telegram's special "secret" chats use end-to-end encryption, leaving no trace of the chat's on Telegram's servers. The secret chats provide users the option to self-destruct messages and prohibit users from forwarding the messages. When users set the self-destruct timer on secret messages, the messages will disappear from both the sender's and receiver's devices when the timer expires.
57. Telegram users have the option to create a user name that is displayed to other users. User names are uniquely assigned on a first-come, first-serve basis. Users have the ability to conceal their user names from others so that they can utilize Telegram anonymously.
58. Based on my training and experience, I know that individuals involved in child pornography and child abuse offenses have utilized Telegram Messenger to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of offenders utilize Telegram's security features to avoid detection from law enforcement officers.

FACTS SUPPORTING PROBABLE CAUSE

Information from Cooperating Witness

59. Beginning in or around December 2019, I have been involved in an investigation of child pornography offenses committed by an adult male who will be referred to for purposes of this Affidavit as "Adult Male A". Adult Male A has pled guilty in the United States District Court for the Southern District of Ohio to one count of production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e). As part of his plea agreement, Adult Male A admitted that he had produced child pornography in 2019 and that he had viewed child pornography files depicting other children.
60. As part of the investigation, Adult Male A was interviewed on two occasions in March 2020 and May 2020. During these interviews, Adult Male A identified that he had received child

pornography files from an individual who lived in Troy, Ohio. During the first interview, Adult Male A referred to this individual as "WILLIAM" and advised that WILLIAM's last name might be HITCHINGS or HIGGINS. During the second interview, Adult Male A advised that this individual's name was either "WILL HIGGINS" or "WILL HITCHINGS".

- a. I know, based on my training and experience, that WILL is a common nickname for WILLIAM. It is common, in my experience, for individuals to transpose nicknames with true names.
- b. Based on the information Adult Male A provided about the individual who sent him the child pornography, there is probable cause to believe that Adult Male A was referring to HITCHINGS.

61. During the first interview in March 2020, Adult Male A minimized his involvement in child pornography activities. He only admitted that he received and viewed child pornography on a limited number of occasions, and he denied that he produced child pornography. Below is a summary of information that Adult Male A provided about HITCHINGS during the first interview:

- a. Adult Male A reported that he received at least one video depicting child pornography from HITCHINGS on a past occasion. HITCHINGS sent this video to Adult Male A via Telegram. Adult Male A acknowledged that there may have been additional occasions in which HITCHINGS sent him (Adult Male A) child pornography files.
- b. Adult Male A stated that he did not want to get HITCHINGS in trouble, but that HITCHINGS was "into" child pornography.
- c. Adult Male A had been to HITCHINGS' residence in the past. Adult Male A saw HITCHINGS view child pornography and bestiality files on a computer that was in HITCHINGS' residence.
- d. HITCHINGS had a large rack of computers inside of his residence.
- e. Adult Male A described HITCHINGS' residence as being on State Route 41 (also known as Main Street) near a school in Troy, Ohio.

62. Adult Male A was interviewed again in May 2020 pursuant to his arrest. During this interview, Adult Male A admitted that he had produced, received, and distributed child pornography files. He also provided additional information about HITCHINGS during this interview. Below is a summary of information that Adult Male A provided about HITCHINGS during the second interview:

- a. On the first occasion that Adult Male A was at HITCHINGS' residence, HITCHINGS took Adult Male A into the basement. HITCHINGS had a black rack of computers in the basement. HITCHINGS asked if Adult Male A wanted to see some "crazy" videos and then proceeded to show Adult Male A videos depicting bestiality and child pornography.
 - b. Over one year ago, HITCHINGS gave Adult Male A a desktop computer that was "packed" full of child pornography and adult pornography files. The pornography included children having sex with other children and animals. Adult Male A later destroyed the hard drive that was in this desktop computer.
 - c. HITCHINGS also at one time gave Adult Male A a laptop computer that contained child pornography files.
 - d. HITCHINGS previously told Adult Male A that there was good child pornography on Telegram.
 - e. Adult Male A again described HITCHINGS' residence as being on State Route 41 near a school and where the road curved. Adult Male A identified that HITCHINGS lived with his boyfriend, CHRIS (no last name provided), and HITCHINGS' mother.
63. It was noted that during both of the interviews of Adult Male A, he sometimes talked about how his deceased relatives and God spoke to him. However, Adult Male A provided information about his child pornography activities that was consistent with other information obtained pursuant to the investigation, including information provided by victims and cooperating witnesses, information obtained from Adult Male A's electronic accounts pursuant to search warrants, and other information obtained pursuant to the investigation. It is therefore reasonable to believe that the information Adult Male A provided about HITCHINGS is credible.
64. It was also noted that Adult Male A provided more information about his own child pornography activities as well as HITCHINGS' child pornography activities during the second interview (which was conducted pursuant to Adult Male A's arrest). Based on my training and experience, I know that it common for individuals to withhold information about their criminal activities when first contacted by law enforcement officers. Individuals often withhold such information as a means to protect themselves and their co-conspirators from criminal culpability. It is not uncommon for such individuals to be more truthful during subsequent interviews when they are faced with additional evidence and/or during interviews conducted after they have been arrested.

Cyber Tipline Report

65. As part of the investigation, I have learned that Synchronoss Technologies Inc. filed a report to NCMEC's Cyber Tipline on or around November 23, 2020, regarding approximately six suspected child pornography or child exploitation files located in a Verizon Cloud account associated with telephone number 937-554-7700 (hereinafter referred to as the "TARGET CELL PHONE"). Synchronoss Technologies Inc. provided these approximately six suspected child pornography or child exploitation files to NCMEC as part of its Cyber Tipline report.
66. NCMEC forwarded Synchronoss Technologies Inc.'s Cyber Tipline report, along with the suspected child pornography or child exploitation files, to me for further investigation. Based on my review of the files and my training and experience, I believe that approximately six of the files depict child pornography. By way of example, three of the files are described as follows:
- a. a968ea8e58fa4b458ed2f98b600f626f_file1.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white male child who is lying on his back with his legs spread apart, exposing his nude genitals to the camera. What appears to be an adult white male (whose face is not captured in the image) appears to be urinating on the child.
 - b. a968ea8e58fa4b458ed2f98b600f626f_file2.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white male child performing fellatio on what appears to be an adult white male (whose face is not captured in the image).
 - c. a968ea8e58fa4b458ed2f98b600f626f_file3.jpg: The file is an image that depicts what appears to be two nude pre-pubescent white male children who are standing next to each other. One child is touching the other child's penis.

Records Obtained Pursuant to Search Warrants and Subpoenas

67. On or around January 12, 2021, Verizon was served with a search warrant requesting information associated with the TARGET CELL PHONE (including historical cell site records) for the time period of January 1, 2020 through January 12, 2021. Records received from Verizon in response to the search warrant provided the following information:
- a. The TARGET CELL PHONE was subscribed to CHRISTOPHER SWEENEY (hereinafter referred to as "SWEENEY") at 924 East Main Street in Troy, Ohio (hereinafter referred to as the "SUBJECT PREMISES"). The contact person listed for the account was HITCHINGS. HITCHINGS' address was also listed as being the SUBJECT PREMISES.
 - i. Based on my training and experience, I know that individuals' telephone

accounts may be subscribed to in other persons' names for a variety of reasons. One such reason could be that the individual has poor credit. Another reason could be that the person is on a "family plan" with a relative(s) or friend(s). Yet another reason could be to conceal the person's identity when the telephone account is being used in furtherance of illegal activities.

- b. The device that utilized the TARGET CELL PHONE was a Motorola Moto z3 cellular telephone.
- c. The historical cell site records for the TARGET CELL PHONE identified that it was consistently in the area of the SUBJECT PREMISES, including during overnight hours.

68. On or around January 12, 2021, Synchronoss Technologies Inc. was served with a search warrant requesting the account contents of the Verizon Cloud account associated with the TARGET CELL PHONE. The account contents provided by Synchronoss Technologies Inc. in response to the search warrant included approximately seven documents, approximately 1,647 image files, and approximately 90 video files. Below is a summary of information noted regarding these files:

- a. More than 450 of the image and video files depicted a male who appears to be HITCHINGS. These files included the following:
 - i. A number of the images and videos depicted HITCHINGS engaged in sexually explicit conduct. Some of the images and videos depicted HITCHINGS engaged in sexually explicit conduct with a dog.
 - ii. A number of the images and videos depicted HITCHINGS in what appears to be a basement. Numerous computer and electronic media (including computers, computer servers, computer hardware, and surveillance systems) were depicted in the images and videos of HITCHINGS.
 - 1. As noted above, Adult Male A reported that HITCHINGS had a large rack of computers in his basement.
 - iii. The EXIF data and metadata for the images and videos indicated that they were produced during the approximate time period of 2013 through 2020.
 - iv. The EXIF data indicated that the following devices were utilized to produce the images: Motorola Moto z3 (the device associated with the TARGET CELL PHONE), a GoPro Hero 4, an LGE Nexus 4 cellular telephone, an LG

Model LG-918 cellular telephone, a Kyocera Model E6830 cellular telephone, and nine different models of Samsung cellular telephones.

- v. One image depicted HITCHINGS' Ohio driver's license.
- b. One image depicted a screen print of what appears to be an order confirmation from an Internet-based purchase. This order confirmation listed HITCHINGS' name as the recipient along with the SUBJECT PREMISES.
- c. Approximately three images depicted three packages from the United States Postal Service and United Parcel Service, all of which were addressed to HITCHINGS at the SUBJECT PREMISES. Approximately one image depicted a Packing List for an order, with HITCHINGS' name and the SUBJECT PREMISES listed as the recipient of the items on the document.
- d. In addition to the images and videos depicting HITCHINGS with computer devices, numerous other images and videos depicted computer and electronic media – including computers, computer servers, computer hardware, and surveillance systems. Some of the images depicted what appears to be monitoring screens for the surveillance cameras. Based on these images as well as other information obtained pursuant to the investigation, it appears that there were surveillance cameras that capture both the interior and exterior of HITCHINGS' residence, and that monitoring screens for these cameras were located both in the basement as well as the Living Room of the residence.
- e. One image depicted what appears to be a screen print from an Internet website. This screen print listed the email address of **w.hitchings@gmail.com**.
- f. Approximately eight of the images depicted what appears to be child pornography. Six of these files were the same as those reported in the Cyber Tipline report filed by Synchronoss Technologies Inc. (as detailed above). The other two files are described as follows:
 - i. Felixxx_134931EdF_koz.jpg: The file is an image that depicts what appears to be a nude toddler-aged male child. The child's legs are straddled, exposing his nude genitals and anus to the camera. It appears that the child's legs are bound to his arms with black tape. What appears to be an adult white male (whose face is not captured in the image) is pointing his penis toward (or possibly touching his penis to) the child's leg and penis.
 - ii. Felixxx_143309iCO_6598.jpg: The file is an image that depicts what appears to be a pre-pubescent white male child. The child is turned upside

down over the lap of what appears to be an adult white male (whose face is not captured in the image). The child's pants are pulled down, exposing his nude genitals and anus to the camera. The adult male's hands are touching the child's legs and buttocks. The adult male's penis is exposed and pointed over the child's buttocks.

- g. Approximately two of the images depicted what appears to be nude pre-pubescent male children.
- h. At least approximately 22 of the images and videos depicted substances that, based on my training and experience, appear to be controlled substances. These files included the following:
 - i. Approximately 10 of the images and videos depicted a green leafy substance that appears consistent with marijuana. In one of the images, the substance was contained in a foil pan placed on a scale, with the scale showing a weight of 1.69 ounces.
 - ii. Approximately four of the images and videos depicted a crystal rocky substance that appears consistent with methamphetamine. One of these images depicted the crystal substance in a Tupperware container on a scale, with the scale showing a weight of 26.21 grams.
 - iii. Approximately five of the images and videos depicted a white rocky substance that appears consistent with crack cocaine or methamphetamine. Approximately two of the images depicted the substance in bags on a scale, with the scale showing weights of 2.04 grams and 0.79 grams.
 - iv. Approximately three videos depicted an individual smoking a substance from a bong.
 - v. The EXIF data for the images identified that they were produced with a Motorola Moto z3 cellular telephone (the device associated with the TARGET CELL PHONE) during the approximate time period of August 1, 2019 through November 1, 2020. The background shown in some of the images and videos appear to match the background of the basement where HITCHINGS was captured in other images and videos (as detailed above).
- i. One of the documents had a title on the first page of the following: "Dome Network Camera Quick Start Guide". This document provided instructions on how to use a dome surveillance camera. Another document was entitled "Family Fun". This document required a password to access it, and as such, could not be viewed.

69. Based on the information contained in the Verizon Cloud account as well as other information detailed in the Affidavit, it appears that HITCHINGS has had access to numerous computer devices. It also appears that HITCHINGS has had access to controlled substances. Based on my training and experience, the drug paraphernalia depicted in some of the images and videos (such as the scales and packaging materials) as well as the quantities and weights of some of the substances are consistent with someone who distributes controlled substances.
70. On or around January 14, 2021, an administrative subpoena was served to Google LLC requesting subscriber information for the **w.hitchings@gmail.com** Google account, as well as logs of IP addresses utilized to access the account. Records received in response to the subpoena provided the following information:
- a. The account was created on or around September 12, 2004 in the name of "WILLIAM HITCHINGS".
 - b. The alternate email address listed for the account was **wenglebot@yahoo.com**. The sign-in telephone number for the account as well as the recovery telephone number for the account were both listed as being the TARGET CELL PHONE.
 - i. Based on my training and experience, I know that many email providers such as Google LLC ask their users to provide alternate or recovery email addresses and telephone numbers when signing up for email accounts. The email providers send various notifications regarding the use of the users' email accounts to the alternate email addresses and telephone numbers to serve as security measures (i.e., to ensure that users' accounts have not been hacked or otherwise compromised). The email provider may also send to the user's alternate account a verification code that is needed to change a password to the user's account or complete another type of account maintenance.
 - c. Services associated with the account included (among others) Gmail, Google Hangouts, Google Drive, Google Maps, Google Photos, Location History, and Web and Application Activity.
 - d. The most recent login for the account was on or around January 11, 2021.
71. As part of the investigation of Adult Male A, records were obtained pursuant to search warrants for various telephone numbers that he utilized as well as for his Facebook account (a social media website administered by Facebook Inc.). Consistent with the information provided by Adult Male A regarding his relationship with HITCHINGS, these records provided the following information:

- a. Records obtained from AT&T for one of the telephone numbers utilized by Adult Male A identified that during the approximate time period of October 2018 through March 2019, Adult Male A exchanged approximately 16 telephone calls and 233 text messages with the TARGET CELL PHONE.
- b. Records obtained from Facebook Inc. for Adult Male A's Facebook account identified that as of the date that the records were produced (in or around February 2020), an account with a profile name of "WILLIAM HITCHINGS" was on Adult Male A's "blocked" Friends list.
 - i. On or around January 11, 2021, I attempted to access the "WILLIAM HITCHINGS" Facebook account. The account is currently disabled, and no publicly available information was available.

Records Obtained from Public Records

- 72. Based on review of a police report of the West Milton (Ohio) Police Department, I learned that on or around January 15, 2017, a police officer was dispatched to a residence in West Milton, Ohio. The occupant reported that his son had located an abandoned cellular telephone on a nearby street. This abandoned cellular telephone was turned over to the officer. The officer thereafter received a telephone call from HITCHINGS, who reported that he was the owner of the abandoned telephone. The officer requested that HITCHINGS provide proof that he was the owner of the telephone. A few weeks later, an officer released the telephone to HITCHINGS (although the report did not detail what proof, if any, that HITCHINGS provided that he was the owner of the telephone). HITCHINGS signed a property receipt for the telephone. On this receipt, he identified that his telephone number was the TARGET CELL PHONE.
- 73. Records from the Ohio Bureau of Motor Vehicles identified that HITCHINGS utilized the SUBJECT PREMISES (the address associated with the TARGET CELL PHONE) on his current Ohio driver's license. Records from the Ohio Bureau of Motor Vehicles identified that HITCHINGS also utilized the SUBJECT PREMISES when registering a motor vehicle.
 - a. I have driven by the SUBJECT PREMISES, and I noted that its location is consistent with the description provided by Adult Male A of HITCHINGS' residence.
- 74. Records from the Miami County (Ohio) Auditor's website identified that SWEENEY presently owns the SUBJECT PREMISES. Records from the Ohio Bureau of Motor Vehicles identified that SWEENEY also utilized the SUBJECT PREMISES on his current Ohio driver's license.
 - a. As detailed above, Adult Male A identified that HITCHINGS resided with his boyfriend, whose first name was "CHRIS".

Review of Social Media Accounts

75. On or around January 5 and 14, 2021, an FBI investigator reviewed publicly available information on various social media websites and messenger applications for any possible accounts associated with the TARGET CELL PHONE and the email addresses **w.hitchings@gmail.com** and **wenglebot@yahoo.com**. Among other accounts, the analyst located the following:
- a. A Skype account was located that was associated with the email address **w.hitchings@gmail.com**. This Skype account contained a user name of “**o0bc0o**” and a profile name of “WILLIAM”.
 - b. A Dropbox account was located that was associated with the email address **w.hitchings@gmail.com**.
 - c. A Google account was located that was associated with both the email addresses **w.hitchings@gmail.com** and **wenglebot@yahoo.com**. The profile picture for the account depicted a male who appears to be HITCHINGS.
 - d. A Telegram account was located associated with the TARGET CELL PHONE. The account had a display name of “Bee Cee” and a user name of “**o0bc0o**” (the same user name as the Skype account listed above). The account was presently offline.
 - i. As detailed above, Adult Male A identified that he received one or more child pornography files from HITCHINGS via Telegram.

Conclusion Regarding Use of Accounts

76. Based on all of the information detailed in the Affidavit, there is probable cause to believe that HITCHINGS is the user of the following:
- a. The TARGET CELL PHONE and the Verizon Cloud account associated with the TARGET CELL PHONE;
 - b. The Google account associated with the email addresses **w.hitchings@gmail.com** and **wenglebot@yahoo.com**;
 - c. The Yahoo email address **wenglebot@yahoo.com**;
 - d. The Skype account associated with the email address **w.hitchings@gmail.com** and/or the user name of **o0bc0o**; and
 - e. The Dropbox account associated with the email address **w.hitchings@gmail.com**;

Evidence Available in Email and Social Media Accounts

77. Based on my training and experience, I know that individuals involved in child exploitation activities sometimes post pictures and videos of their victims on their social media accounts. Although the pictures and videos posted by the offenders often do not depict child pornography, these files may provide evidentiary value to child exploitation investigations in that they may be partially comparable to the child pornography files (i.e., they may depict the same clothing items, body types, etc.) and/or they may help in identifying the victims.
78. Based on my training and experience, I know that individuals involved in drug offenses often take pictures of their controlled substances and drug paraphernalia. Individuals often post these pictures on their social media accounts, and they sometimes email these pictures to themselves or others.
79. I also know, based on my training and experience, that individuals often post on their social media accounts pictures of their residences, travels, and whereabouts. Individuals also post information and exchange messages regarding their travels and whereabouts. These pictures and postings again may provide evidentiary value to child exploitation and drug investigations in that they may help to identify the locations of the criminal activities.
80. In my experience, individuals often post information on their social media accounts about other electronic accounts that they utilize – including their email addresses, other social media accounts, and messenger accounts. This information may provide evidentiary value to child exploitation and drug investigations in that they help in identifying other accounts utilized by the offenders in furtherance of their child exploitation and drug activities.
81. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
82. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

83. Based on my training and experience, I am aware that individuals involved in drug offenses often communicate with co-conspirators (including suppliers and customers) via e-mail, social media accounts, and online chat programs. Individuals often utilize messenger applications (including messenger applications associated with their social media accounts) to coordinate various aspects of their drug activities (such as purchases and sales).
84. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.
85. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation and drug offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Child exploitation offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Child exploitation offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.
86. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation and drug offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.
87. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child exploitation and drug offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.

88. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography and/or purchase controlled substances, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.
89. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography and drug investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

90. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.
91. Based on my training and experience, I know that individuals involved in drug offenses sometimes conduct Internet searches related to their drug activities, such as the prices of drugs and materials utilized in manufacturing the drugs. The Web and Application history maintained by Google LLC is therefore also materially relevant to drug investigations.
92. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals often back up the photographs and videos on their telephones to their Google Photos account. Therefore, any photographs and videos taken with or stored on users' telephones (including child pornography files and photographs depicting controlled substances) may also be recovered on their Google Drive and Google Photos account. Furthermore, in my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.
93. As noted above, based on my training and experience, I know that individuals involved in drug offenses often take pictures of their controlled substances and drug paraphernalia. It is not uncommon for these types of photographs to be backed up to the individuals' cloud accounts, such as Google Drive and Google Photos.
94. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation

and drug offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

95. As detailed above, Google Location History is an application in which Google utilizes various data such as cell site information and Wi-Fi routers to locate and geo-locate a cellular telephone device. Google collects and stores this data if the application is enabled by the user, either during the set-up of the device or through the device's settings.
96. Based on my training and experience, I know that location information from cellular telephones and Google accounts can be materially relevant in investigations involving child exploitation and drug offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims and co-conspirators. Data regarding the subjects' whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place. Furthermore, data regarding the subjects' whereabouts as obtained from the location information can lead to the identification of the places where computer devices used in furtherance of the crime may be present.

Evidence Sought in Searches of Dropbox Accounts

97. Dropbox and other cloud storage services provide a means that individuals can use to store files. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.
98. As noted above, based on my training and experience, I know that individuals involved in drug offenses often take pictures of their controlled substances and drug paraphernalia. It is not uncommon for these types of photographs to be backed up to the individuals cloud accounts, such as Dropbox.
99. Based on information received from Dropbox Inc., I know that Dropbox Inc. maintains basic subscriber information for its users, including user names, email addresses, and the dates that they established their accounts. Dropbox Inc. also maintains payment information, including credit card numbers, when payments are made on the accounts. Such information can provide material evidence regarding individuals involved in child pornography and drug offenses, because this information can help identify the subjects and determine what aliases and email accounts they utilize. In addition, the dates that the accounts were established can help in identifying the length of time that the criminal activities transpired.
100. In addition to maintaining the files themselves, Dropbox Inc. also maintains files documenting various activities associated with its accounts. One such file is entitled "uploadlog.html". This file maintains information about the account name, computer name, and dates that files were uploaded, deleted, and modified. Such information provides

material evidence to child pornography and drug investigations, as the information helps identify the computer devices utilized by the subjects and when and how the files were received.

101. Another file maintained by Dropbox Inc. for its accounts is entitled "auth.txt". This file maintains logs of IP addresses and devices utilized to access the account. Such information is important to child pornography and drug investigations because it helps to establish the subjects' identities, what computer devices are utilized, where the subjects' computers are located, and when the criminal activities transpired.
102. A file entitled "links.txt" is another example of a file maintained by Dropbox Inc. for its accounts. This file maintains information about files being shared by the user. In cases involving the trading of child pornography, information about the shared files can be useful in helping to identify the subjects' trading activities.
103. Dropbox Inc. maintains various information about the settings for its users' accounts. Such settings include information about computers and other devices linked to the accounts. Information about what computers and devices are utilized by the subjects is again materially important to child pornography investigations.

Conclusion Regarding Probable Cause

104. Based on all of the information detailed above, there is probable cause to believe the following:
 - a. HITCHINGS has used one or more computer devices (including the TARGET CELL PHONE) to possess, receive, and distribute child pornography files.
 - b. HITCHINGS has possessed controlled substances.
 - c. The Verizon Cloud account associated with the TARGET CELL PHONE contains evidence of HITCHINGS' child pornography and drug activities.
 - d. The Google accounts associated with the email addresses **w.hitchings@gmail.com** and **wenglebot@yahoo.com** may contain evidence of HITCHINGS' child pornography and drug activities. This evidence potentially includes email messages providing evidence of other possible social media and messenger accounts utilized by HITCHINGS in furtherance of his child pornography and drug activities, email messages providing evidence of the identity of the user of the associated accounts, Web and Application history providing evidence of Internet searches conducted in furtherance of his child pornography and drug activities, images and videos depicting child pornography and/or controlled substances saved in the Google Photos or Google Drive accounts, and/or location information that may lead to the identification of HITCHINGS' child pornography and drug activities.

- e. The email address **wenglebot@yahoo.com** may contain evidence of HITCHINGS' child pornography and drug activities. This evidence potentially includes email messages providing evidence of other possible social media and messenger accounts utilized by HITCHINGS in furtherance of his child exploitation and drug activities and email messages providing evidence of the identity of the user of the associated accounts.
- f. The Dropbox account associated with the email address **w.hitchings@gmail.com** may contain evidence of HITCHINGS' child pornography and drug activities.
- g. The Skype account associated with email address **w.hitchings@gmail.com** and/or the user name of **o0bc0o** may contain evidence of HITCHINGS' child pornography and drug exploitation activities, including possible communications with other offenders and victims.


ELECTRONIC COMMUNICATIONS PRIVACY ACT

105. I anticipate executing the requested warrants for the listed accounts under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Google LLC, Oath Holdings Inc., Microsoft Corporation, and Dropbox Inc. to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 through B-4. Upon receipt of the information described in Section I of Attachments B-1 through B-4, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-4.

CONCLUSION

106. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; including violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(1), 18 U.S.C. §§ 2252(a)(2) and (b)(1), 18 U.S.C. §§ 2252A(a)(2) and (b)(1), and 21 U.S.C. § 844, are present in the information associated with the above noted accounts (as described in Attachments A-1 through A-4).
107. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-4.
108. Because the warrants for the accounts described in Attachments A-1 through A-4 will be served on Google LLC, Oath Holdings Inc., Microsoft Corporation, and Dropbox Inc., who

will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 19th of January 2021


Sharon L. Ovington
United States Magistrate Judge

